

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

1-8 (Canceled)

1 9. (Previously presented) A computer-implemented method for ensuring
2 non-repudiation of a payment request, the payment request being generated in a computing
3 environment having a connection to a network, the method comprising the steps of:
4 receiving, over the network, the payment request together with a certificate
5 identifying a user having caused the payment request to be generated, the certificate including
6 certificate-identifying information and user-identifying information, the certificate further
7 including authority information defining an authority of the user to make the payment request,
8 the authority information including a maximum payment that the user is authorized to make and
9 an identification of payees to whom the user is authorized to make payments;
10 validating the certificate-identifying information and the user-identifying
11 information included within the received certificate;
12 accessing a store of authority information that is coupled to the network, that is
13 stored apart from the payment request and that is independent of the received certificate;
14 retrieving, from the accessed store of authority information, stored authority
15 information that is associated with the user;
16 comparing the retrieved authority information with the authority information
17 included within the received certificate to determine whether the retrieved authority information
18 matches the authority information included within the received certificate;
19 validating the authority information within the received certificate only if the
20 retrieved authority information matches the authority information included within the received
21 certificate, and

22 executing of the payment request only when the certificate-identifying
23 information, the user-identifying information and the authority information within the received
24 certificate is successfully validated.

1 10. (Original) The method of claim 9, wherein the payment request is for a
2 predetermined amount and wherein the payment request is authorized only when the validating
3 steps are successful and when the authority information for the user stored in the hierarchical
4 authority data structure lists an authorized amount for the user at least equal to the predetermined
5 amount.

1 11. (Original) The method of claim 9, wherein the certificate received in the
2 receiving step conforms to the X.509 standard.

1 12. (Original) The method of claim 9, wherein the authority information is
2 configured as XML code.

1 13. (Original) The method of claim 9, wherein the XML code is compliant
2 with a DSML standard.

14. (Canceled)

1 15. (Previously presented) A computer-readable storage medium configured
2 to store one or more software application configured to carry out a financial transaction, the
3 application being configured to run on a computer coupled to a network, the computer-readable
4 storage medium comprising:
5 certificate receiving code which is configured to receive a digital certificate from
6 a user over the network, the certificate including certificate-identifying information and user-
7 identifying information, the certificate further including authority information that defines an
8 authority granted to the user to request that the financial transaction be carried out, the authority
9 information including a maximum payment that the user is authorized to make and an
10 identification of payees to whom the user is authorized to make payments;

11 certificate validating code configured to enable validation of the certificate-
12 identifying information and user-identifying information within the received certificate, and
13 authorization validating code configured to cause the computer to carry out steps
14 of:

15 accessing a store of authority information that is coupled to the network,
16 that is stored apart from the payment request and that is independent of the received certificate;
17 retrieving, from the accessed data structure, stored authority information
18 that is associated with the user;
19 comparing the retrieved authority information with the authority
20 information included within the received certificate to determine whether the retrieved authority
21 information matches the authority information included within the received certificate;
22 validating the authority information within the received certificate only if
23 the retrieved authority information matches the authority information included within the
24 received certificate, and
25 executing of the financial transaction only when the authority information
26 within the received certificate is successfully validated.

1 16. (Previously presented) The computer-readable storage medium of claim
2 15, wherein the digital certificate conforms to the X.509 standard.

1 17. (Previously presented) The computer-readable storage medium of claim
2 15, wherein the authority information is configured as XML code.

1 18. (Previously presented) The computer-readable storage medium of claim
2 17, wherein the XML code is compliant with a DSML standard.

1 19. (Previously presented) The computer-readable storage medium of claim
2 15, wherein the authority defined by the authority information within the received certificate also
3 defines rights of the user to access predetermined data and programs within the network.

20-28 (Canceled)

1 29. (Previously presented) A server computer to authenticate a user of a client
2 computer and to verify that the user is authorized to request that the server computer carry out a
3 requested action, the server computer comprising:

4 a processor; and

5 a memory coupled to the processor and configured to store a set of instructions
6 that when executed by the processor causes the processor to:

7 receive a payment request along with a digital certificate assigned to the
8 user of the client computer, the digital certificate comprising a first code portion and a second
9 code portion,

10 wherein the first code portion of the digital certificate is configured
11 to enable authentication of the user, the first code portion defines a public key, a certificate serial
12 number, a certificate validity period, a digital signature of the certificate authority, and an
13 extension field,

14 wherein the second code portion of the digital certificate is
15 configured to define an authority of the user of the client computer to request that the server
16 computer carry out the requested action, the second code portion being configured for inclusion
17 within the extension field of the first code portion, the authority of the user defined within the
18 second code portion of the certificate defining access rights of the user including a maximum
19 payment that the user is authorized to make and an identification of payees to whom the user is
20 authorized to make payments;

21 access a store of authority information that is coupled to the network, that
22 is stored independent of the received digital certificate;

23 retrieve, from the accessed store of authority information, authority
24 information that is associated with the user of the client computer;

25 compare the retrieved authority information with the authority information
26 included within the digital certificate to determine whether the retrieved authority information
27 matches the authority information included within the digital certificate;

28 validate the authority information within the digital certificate only if the
29 retrieved authority information matches the authority information included within the digital
30 certificate, and
31 carry out the requested action only when the authority information within
32 the digital certificate is successfully validated.

1 30. (Previously presented) The server computer of claim 29, wherein the
2 digital certificate conforms to the X.509 standard.

1 31. (Previously presented) The server computer of claim 2.9, wherein the
2 second code portion is configured as XML code.

1 32. (Previously presented) The server computer of claim 31, wherein the
2 XML code is compliant with a DSML standard.

1 33. (Previously presented) The server computer of claim 29, wherein the
2 authority of the user of the client computer is stored in a hierarchical authority data structure that
3 is accessible by the server computer.